512.74
T22u

Ueber die $\frac{p-1}{2}$ gliedrigen Gaussischen Perioden

in der Lehre von der Kreisteilung und ihre Beziehungen zu anderen Teilen der höheren Arithmetik.

Inaugural-Dissertation

zur Erlangung der Doctorwürde

der hohen philosophischen Fakultät
der Königl. Christian-Albrechts-Universität zu Kiel

vorgelegt von

Hermann Teege
aus Schackendorf (Holstein).

NOTICE: **Return or renew all Library Materials! The *Minimum* Fee for each Lost Book is $50.00.**

The person charging this material is responsible for its return to the library from which it was withdrawn on or before the **Latest Date** stamped below.

Theft, mutilation, and underlining of books are reasons for disciplinary action and may result in dismissal from the University.
To renew call Telephone Center, 333-8400

UNIVERSITY OF ILLINOIS LIBRARY AT URBANA-CHAMPAIGN

OCT 0 3 1994

JUL 28 RECT

L161—O-1096

UNIVERSITY OF
ILLINOIS LIBRARY
AT URBANA-CHAMPAIGN
MATHEMATICS

Ueber die $\frac{p-1}{2}$ gliedrigen Gaussischen Perioden in der Lehre von der Kreisteilung und ihre Beziehungen zu anderen Teilen der höheren Arithmetik.

Inaugural-Dissertation

zur Erlangung der Doctorwürde

der hohen philosophischen Fakultät
der Königl. Christian-Albrechts-Universität zu Kiel

vorgelegt von

Hermann Teege
aus Schackendorf (Holstein).

Opponenten:

Herr **J. Ehrichsen**, Dr. phil.
Herr **H. Bahrdt**, Assistent am physik. Institut.
Herr **K. Glatzer**, cand. phil.

KIEL.
Druck von P. Peters.
1900.

No. 17.
Rektoratsjahr 1899/1900.
Zum Druck genehmigt:
Prof. Dr. Hasbach,
z. Z. Decan.

512.74
512.81
T224

Seiner lieben Mutter

in Dankbarkeit gewidmet.

SIMMONS
1085605

Digitized by the Internet Archive
in 2022 with funding from
University of Illinois Urbana-Champaign

https://archive.org/details/ueberdiep12glied00teeg

In seinem monumentalen Werke, den Disquisitiones arithmeticae, giebt *Gauss* zwei im wesentlichen verschiedene Methoden, nach denen die binomischen Gleichungen, oder wie man sie auch mit Rücksicht auf ihre geometrische Anwendung zu nennen pflegt, die Kreisteilungsgleichungen von der Form

$$x^p - 1 = 0$$

aufgelöst werden können. Nach der einen, der hauptsächlich der ganze siebente Abschnitt der Disquisitiones arithmeticae gewidmet ist und die daher speciell als die Gaussische Methode bezeichnet worden ist, wird die Auflösung der Kreisteilungsgleichung

$$x^p - 1 = 0,$$

wo p eine Primzahl ist, mit Hilfe der sogenannten Gaussischen Perioden auf die Auflösung je einer Gleichung vom Grade m_1, m_2, m_3 . . . . . zurückgeführt, wo die Zahlen m die gleichen oder verschiedenen in p—1 aufgehenden Primzahlen bedeuten, so dass $p-1 = m_1 . m_2 . m_3 \ldots$ ist. Auch wird darauf hingewiesen, dass diese Gleichungen zwar stets algebraisch, d. h. durch Wurzelgrössen lösbar sind, dass sie aber auf keine andere Weise vermieden oder auf Gleichungen von niedrigerem Grade zurückgeführt werden können. Dadurch wird jede Hoffnung, den Kreis mit Hilfe von Zirkel und Lineal auch noch in anderen Fällen zu teilen, als wenn p von der Form $2^n + 1$ ist, für immer zerstört; dagegen erledigt die Gaussische Methode diesen Specialfall in einer Weise, die nichts zu wünschen übrig lässt. Namentlich die Teilung des Kreises in 17 gleiche Teile, die der damals noch nicht 20 jährige junge Mathematiker auf elementar-geometrischem Wege auszuführen lehrte, erregte allgemeines Aufsehen und machte den Namen des Entdeckers mit einem Male bekannt und berühmt, nachdem man in 2000 Jahren über den Standpunkt Euklids nicht hinausgekommen war; denn sämtliche Mathematiker hatten an die Möglichkeit anderer Teilungen als in 2, 3 oder 5

gleiche Teile, wie sie schon den alten Griechen bekannt gewesen waren, nicht im entferntesten gedacht oder sie gar ausdrücklich in Abrede gestellt.

Die zweite der oben erwähnten Methoden findet sich in den Disquisitiones arithmeticae nur angedeutet und ist später von *Cauchy, Eisenstein* und namentlich *Jacobi* wesentlich vervollkommnet worden. Es muss jedoch bemerkt werden, dass schon vor den Veröffentlichungen dieser Männer *Gauss* zu ganz ähnlichen Resultaten gelangt war, wie aus einer Abhandlung: Disquisitionum circa aequationes puras ulterior evolutio zu ersehen ist, welche zwar erst nach seinem Tode gedruckt, aber bereits im Jahre 1808 niedergeschrieben worden ist. Diese Methode bedient sich der Lagrange'schen Resolventen zur Lösung der Kreisteilungsgleichungen und führt das Problem in letzter Linie zurück auf die Bildung der von *Jacobi* mit $\Psi_n(\omega^k)$ bezeichneten complexen Zahlen. Diese Methode besitzt wesentliche Vorzüge vor der Gaussischen, namentlich geschieht die Bildung der Funktionen Ψ nach einem sehr einfachen Algorithmus, sodass die numerische Berechnung nicht wie dort eine ganz besondere, wegen ihrer grossen Mühsäligkeit selbst für kleinere Primzahlen nicht mehr ausführbare Arbeit verursacht. Namentlich *Jacobi* hat sich bemüht, diese Methode auf die Zahlentheorie, deren inniger Zusammenhang mit der Lehre von der Kreisteilung ja bekannt ist, zu übertragen, und bei ihrer grossen Allgemeinheit konnte es nicht fehlen, dass eine reiche Ernte auf diesem noch ganz unangebauten Felde seine Mühe lohnte. Kein Wunder daher, wenn die Späteren seinem Beispiele folgten, und zahlentheoretische Untersuchungen, die sich innerhalb der Betrachtungsweise der ersten Gaussischen Methode hielten, sehr vereinzelt blieben.

Viel mag zu dieser Erscheinung auch der Umstand beigetragen haben, dass wegen des Fehlens einer allgemeinen Methode wohl viele einzeln stehende Resultate gewonnen werden konnten, diese aber wegen der Schwierigkeit der Verallgemeinung vielfach nur zusammenhangslose Thatsachen bleiben mussten. Auch den folgenden Untersuchungen, die sich ausschliesslich auf die $\frac{p-1}{2}$ gliedrigen Gaussischen Perioden erstrecken, haftet dieser Mangel an, und

man möge es ihnen daher zu gute halten, wenn nicht an allen Stellen die verknüpfenden Beziehungen aufgefunden werden konnten. Es fehlt der Zahlentheorie fast bis zur charakteristischen Unterscheidung der wesentliche Vorzug der Analyse, dass das Allgemeine wie das Besondere mit gleicher Leichtigkeit erledigt wird.

Die folgende Arbeit zerfällt in zwei Abschnitte. In dem ersten wird zunächst eine neue Methode gegeben, das Vorzeichen der sogenannten Gaussischen Summen zu bestimmen, und dann dieselbe Methode zur Vereinfachung eines früheren von *Kronecker* gegebenen Beweises benutzt; in dem zweiten Abschnitte folgen einige Anwendungen auf die Zahlentheorie und die Lehre von der Kreisteilung.

Die benutzte Litteratur ist überall aus den Fussnoten ersichtlich. Für die geschichtlichen Angaben habe ich mich vielfach auf die einleitenden Bemerkungen in den betreffenden Abhandlungen stützen können; für einen Litteraturnachweis aus neuester Zeit bin ich Herrn Prof. *Dr. Stäckel* zu grossem Danke verpflichtet.

I. Abschnitt.

Die $\frac{p-1}{2}$ gliedrigen Perioden und die Gaussischen Summen.

1.

Bekanntlich gelangt man zu den $\frac{p-1}{2}$ gliedrigen Gaussischen Perioden auf folgende Weise. Ist

$$x^p - 1 = 0$$

die Kreisteilungsgleichung, wo p eine ungerade Primzahl bedeutet, so lassen sich ihre p—1 primitiven Wurzeln in die beiden Gruppen ordnen

$$r^{g^2},\ r^{g^4},\ r^{g^6} \ldots\ r^{g^{p-1}} \text{ und}$$

$$r^{g^1},\ r^{g^3},\ r^{g^5} \ldots\ r^{g^{p-2}},$$

wo $r = e^{\frac{2\pi i}{p}} = \cos\frac{2\pi}{p} + i\sin\frac{2\pi}{p}$ gesetzt ist und g eine primitive Wurzel der Congruenz

$$x^{p-1} \equiv 1 \pmod{p}$$

bedeutet.

Für die erste Gruppe kann man abgesehen von der Reihenfolge

$$r^{a_1},\ r^{a_2},\ r^{a_3} \ldots$$

schreiben, wo $a_1, a_2, a_3 \ldots$ ein vollständiges System quadratischer Reste nach dem Modulus p bezeichnen oder das Legendresche Symbol $\left(\frac{a_1}{p}\right) = \left(\frac{a_2}{p}\right) = \left(\frac{a_3}{p}\right) = \ldots = 1$ ist, und für die zweite Gruppe

$$r^{b_1},\ r^{b_2},\ r^{b_3}\ \ldots$$

wo die b die quadratischen Nichtreste bedeuten, also das Legendresche Symbol $(\frac{b}{p}) = -1$ ist.

Ist p keine Primzahl, sondern eine ungerade zusammengesetzte Zahl P ohne quadratischen Teiler, so werden die beiden Gruppen entsprechend

$$r^{a_1},\ r^{a_2},\ r^{a_3}\ \ldots\ldots$$
$$\text{und } r^{b_1},\ r^{b_2},\ r^{b_3}\ \ldots\ldots,$$

wo das Jacobische Symbol

$$(\tfrac{a_1}{p}) = (\tfrac{a_2}{p}) = (\tfrac{a_3}{p}) = \ldots\ldots = 1 \text{ und}$$
$$(\tfrac{b_1}{p}) = (\tfrac{b_2}{p}) = (\tfrac{b_3}{p}) = \ldots\ldots = -1 \text{ ist,}$$

sodass also die Zahlengruppen der a und der b ein vollständiges System relativer Primzahlen zu P umfassen.

Mit Hülfe der Theorie der Kreisteilung findet man nun leicht, dass im allgemeinen Fall, worin auch der Fall einer Primzahl eingeschlossen ist, die Summe der obigen Gruppen

$\frac{1}{2}\left(-1+\varepsilon i^{(\frac{P-1}{2})^2}\sqrt{P}\right)$, resp. $\frac{1}{2}\left(-1-\varepsilon i^{(\frac{P-1}{2})^2}\sqrt{P}\right)$ beträgt; ε bedeutet das nicht näher zu bestimmende positive oder negative Vorzeichen.

Zusammenfassend kann man endlich schreiben

$$\sum(\tfrac{m}{P})\, e^{m\frac{2\pi i}{P}} = \varepsilon\, i^{(\frac{P-1}{2})^2}\sqrt{P}\ , \qquad (1)$$

wo m ein vollständiges System relativer Primzahlen zu P durchlaufen muss, oder noch allgemeiner

$$\sum(\tfrac{m}{P})\, e^{m\frac{2h\pi i}{P}} = \varepsilon\,(\tfrac{h}{P})\, i^{(\frac{P-1}{2})^2}\sqrt{P} \qquad (2)$$

Endlich ergiebt sich noch leicht

$$\sum e^{m^2 \frac{2h\pi i}{P}} = \varepsilon \left(\frac{h}{P}\right) i^{\left(\frac{P-1}{2}\right)} \sqrt{P}, \qquad (3)$$

wo m ein vollständiges Restsystem nach dem Modulus P durchlaufen muss (mit Einschluss der Zahl $\equiv$ o).

Die Schwierigkeit besteht also nicht in der Bestimmung des absoluten Wertes der obigen Summenausdrücke, die kurz als die Gaussischen Summen bezeichnet werden, sondern in der Bestimmung des Vorzeichens ε. Eine ähnliche Unbestimmtheit findet häufig in der Mathematik statt, lässt sich aber für gewöhnlich leicht beseitigen, indem aus der Natur der zu bestimmenden Grösse leicht erhellt, ob ihr das positive oder negative Zeichen zukommt. Im vorliegenden Falle versagt aber dies Mittel ganz und gar, und es bleibt zunächst kein anderer Weg übrig, als in jedem einzelnen Falle vermittelst der den Tafeln zu entnehmenden Werte für die trigonometrischen Funktionen zur numerischen Berechnung zu schreiten. Man findet auf diese Weise sofort ein äusserst elegantes und einfaches Resultat: in allen Fällen, in welchen für die Einheitswurzel $e^{\frac{2\pi i}{P}}$ gewählt wird oder allgemein $e^{a\frac{2\pi i}{P}}$, wo $\left(\frac{a}{P}\right) = 1$ ist, muss das Vorzeichen der Wurzelgrössen in den obigen Formeln durchaus positiv genommen werden. Allein die Theorie der Kreisteilung scheint kein Mittel an die Hand zu geben, diese merkwürdige Beziehung auch wirklich zu beweisen. Der tiefere Grund liegt natürlich darin, dass die Analyse bei der Auflösung der Gleichung zwischen den verschiedenen Einheitswurzeln keinen Unterschied macht, sondern alle auf gleiche Weise umfasst. Diese kapitale Schwierigkeit reizte aber gerade Gauss nichts unversucht zu lassen, um sie zu beseitigen; er gesteht aber, dass ihm dies erst nach vielen, durch Jahre hindurch fortgesetzten Versuchen gelungen sei [1]). Er hat der Bestimmung des Vorzeichens eine

[1]) Comment. recent. Societ. Götting. Vol. I, art. 4. Gauss'Werke, Bd. II.

eigene Abhandlung gewidmet: Summatio quarundam serierum singularium, und es gelingt ihm darin, durch äusserst scharfsinnige und merkwürdige Betrachtungen die Gültigkeit des Satzes auch für den allgemeinen Fall beliebiger ungerader Zahlen auf direktem Wege zu erbringen. Er benutzt dann das gewonnene Resultat zu einem neuen Beweise des berühmten Reciprocitätsgesetzes in der Lehre von den quadratischen Resten. Nach ihm hat Dirichlet in der Abhandlung: Über eine neue Anwendung bestimmter Integrale auf die Summation endlicher und unendlicher Reihen[1]) und in vereinfachter Gestalt in den Recherches sur diverses applications de l'analyse infinitésimale à la théorie des nombres[2]) den Gegenstand wieder aufgenommen und die Frage durch sehr feine Betrachtungen aus der Lehre von den bestimmten Integralen in einer Weise erledigt, die in bezug auf Allgemeinheit und Übersichtlichkeit nichts zu wünschen übrig lässt. Dann hat in neuerer Zeit *Kronecker* einen dritten direkten Beweis für den allgemeinen Fall gegeben; in einer Abhandlung: Summierung der Gaussischen Reihen

$$\sum_{h=0}^{h=\nu-1} e^{\frac{2h^2\pi i}{\nu}}$$

im 105. Bande des Journals für die reine und angewandte Mathematik zeigt er, wie man mit Hilfe des Cauchyschen Theorems, wonach

$$\int f(x+iy)\ d(x+iy) = 0$$

wird, wenn man die Integration über die Umgrenzung eines Gebietes erstreckt, innerhalb welches die Funktion f und ihre erste Ableitung eindeutig und stetig sind, auf überraschend einfache Weise zur Lösung des Problems der Wertbestimmung der Gaussischen Summen gelangen kann. Endlich hat Herr Prof.

[1]) G. Lejeune Dirichlet's Werke. Herausgegeben auf Veranlassung der Königl. Preuss. Akad. der Wissenschaften von L. Kronecker, Bd. I, pag. 237 u. ff.

[2]) Cr. J. Bd. 19 u. 21. Werke, Bd. I, pag. 473 u. ff.

Fr. Mertens in den Sitzungsberichten der Berliner Akademie der Wissenschaften. Jahrg. 1896, S. 217, einen sehr interessanten Beweis veröffentlicht, der gar keiner besonderen Voraussetzungen mehr bedarf, sondern durch direkte Zerlegung der trigonometrischen Funktionen den positiven Wert der Gaussischen Summen nachweist[1]). Ohne Zweifel muss daher dieser Beweis als der kürzeste und einfachste von allen angesehen werden.

Diese vier direkten Methoden zur Summierung der Reihen für beliebige ungerade Zahlen sind nun, wenigstens soweit mir bekannt, die einzigen, die auf prinzipielle Verschiedenheit und Allgemeinheit Anspruch machen können. Allerdings haben *Cauchy*[2]) und *Lebesgue*[3]) noch zwei Beweise für den allgemeinen Fall veröffentlicht; davon ist aber der eine, der von Lebesgue, mehr als eine Erläuterung des Gaussischen denn als ein neuer selbständiger Beweis anzusehen, und zwischen dem Cauchyschen und dem Dirichletschen Beweise findet, wie Kronecker in einer im Monatsberichte der Berliner Akademie vom Jahre 1880 abgedruckten Abhandlung dargelegt hat, eine innere Übereinstimmung statt. Dagegen giebt es noch zwei andere selbständige Beweise, welche aber direkt nur zur Wertbestimmung der Gaussischen Reihen für den Fall führen, wo p Primzahl ist, zur allgemeinen dagegen nur unter Zuhilfenahme des Reciprocitätsgesetzes in der Lehre von den quadratischen Resten. Der erste dieser Beweise, der ebenfalls von Cauchy angegeben worden ist, findet sich in der schon oben citierten Abhandlung: Méthode simple et nouvelle u. s. w., der andere, der von Kronecker herrührt, ist der Gegenstand einer kleinen Notiz in Liouv. J. Bd. I, 2. série, die den Titel trägt: Sur une formule de Gauss. Beide Beweise haben das Gemeinsame, dass sie sich zur Entscheidung der Frage, welchen der Werte $+1$ oder -1 man für das Vorzeichen zu setzen hat, des Wilsonschen Satzes bedienen, unterscheiden sich aber

[1]) Für diesen Litteraturnachweis bin ich Herrn Prof. P. Stäckel zu Dank verpflichtet.

[2]) Liouv. J. 1840. Bd. V. pag. 154 u. ff.: Méthode simple et nouvelle pour la détermination complète des sommes alternées, formées avec les racines primitives des équations binômes.

[3]) In dems. Bd. d. Liouv. J.: Sommation de quelques séries, pag 42 u. ff.

in der Art der Schlussfolgerungen, durch welche sie die Entscheidung von diesem Satze abhängig machen. Denn während Cauchy sein Augenmerk darauf richtet, was aus einer gewissen Funktion wird, wenn er in ihr statt der h ten Potenz der Einheitswurzel $(\frac{h}{p})$ substituiert, setzt Kronecker für dieselbe Grösse e^z ein und gewinnt sein Resultat durch Vergleichung der Coeffizienten gleich hoher Potenzen zweier Reihenentwicklungen, die nach der Art ihrer Entstehung einander gleich sein müssen.

In die Kategorie der zuletzt erwähnten Beweise ist auch der folgende neue zu rechnen, der namentlich dann von grosser Kürze und Einfachheit wird, wenn er mit dem oben erwähnten Beweise von Kronecker combiniert wird.

2.

Aus der Kreisteilungsgleichung

$$x^p - 1 = 0$$

folgt durch Division mit x—1

$$x^{p-1} + x^{p-2} + x^{p-3} + \ldots + x^2 + x + 1 = 0.$$

p bezeichnet wie immer eine Primzahl.

Die sämtlichen Wurzeln dieser Gleichung sind also

$$r^1,\ r^2,\ r^3,\ \ldots\ r^{p-1},$$

wenn r eine primitive Einheitswurzel bedeutet.

Beachtet man ferner, dass

$$r^0 = r^p = 1$$
$$r^1 = r^{p+1}$$
$$r^2 = r^{p+2}$$

usw.

und $1 = -r^{p-1} - r^{p-2} - r^{p-3} - \ldots - r^2 - r$ ist, so sieht man leicht ein, dass man einen jeden Ausdruck

$$a_0 + a_1 r + a_2 r^2 + a_3 r^3 + \ldots a_n r^n = m$$

auf die sogenannte Normalform

$$A_1r+A_2r^2+A_3r^3+ \ldots A_{p-1}r^{p-1}=m$$

bringen kann, und zwar müssen auch die A ganzzahlig sein, wenn die a ganzzahlig sind. Zu gleicher Zeit ist dies aber auch die einzige Normalform, denn wäre etwa auch

$$B_1r+B_2r^2+B_3r^3+ \ldots B_{p-1}r^{p-1}=m,$$

wo die Coeffizienten B ebenfalls ganzzahlig, aber von den A verschieden sind, so würde man durch Gleichsetzung der beiden Ausdrücke erhalten:

$$(A_1-B_1)r+(A_2-B_2)r^2+(A_3-B_3)r^3+ \ldots (A_{p-1}-B_{p-1})r^{p-1}=0,$$

also eine Gleichung in r mit ganzzahligen Coeffizienten, die von niedrigerem Grade als dem (p—1)ten ist. Dies ist aber wegen der Irreductibilität der Kreisteilungsgleichungen nicht möglich, sodass also auch nur eine einzige Normalform vorhanden sein kann.

Ferner entwickeln wir noch folgende wichtige Beziehung.

Für die Wurzeln der Kreisteilungsgleichungen können auch

$$r^2,\ r^4,\ r^6 \ldots r^{2(p-1)}$$

genommen werden. Demnach ist

$$x^{p-1}+x^{p-2}+x^{p-3}+ \ldots +x^2+x+1=(x-r^2)(x-r^4)(x-r^6) \ldots (x-r^{2(p-1)})$$

oder für x=1

$$p=(1-r^2)(1-r^4)(1-r^6) \ldots (1-r^{2(p-1)}).$$

Multipliziert man auf der rechten Seite je zwei von den Enden gleich weit abstehende Glieder mit einander, so erhält man

$$p=(2-r^2-r^{2(p-1)})(2-r^4-r^{2(p-2)}) \ldots$$

oder

$$p=(-1)^{\frac{p-1}{2}}(r^2+r^{2(p-1)}-2)(r^4+r^{2(p-2)}-2) \ldots,$$

also

$$p=(-1)^{\frac{p-1}{2}}(r-r^{p-1})^2(r^2-r^{p-2})^2(r^3-r^{p-3})^2 \ . \ . \ . \ (r^{\frac{p-1}{2}}-r^{\frac{p+1}{2}})^2.$$

Dieser letzte Ausdruck lässt sich aber leicht wegen

$$r^p=1$$

in

$$p=(-1)^{\frac{p-1}{2}}(2i)^{p-1}\left(\frac{r-r^{-1}}{2i}\right)^2\left(\frac{r^2-r^{-2}}{2i}\right)^2\left(\frac{r^3-r^{-3}}{2i}\right)^2 \ . \ .$$
$$\left(\frac{r^{\frac{p-1}{2}}-r^{-\frac{p-1}{2}}}{2i}\right)^2$$

umformen.

Nimmt man nun für r den Wert $e^{\frac{2\pi i}{p}}$, so erhält man unter Anwendung der Formel

$$\frac{e^{iv}-e^{-iv}}{2i}=\sin v$$

die wichtige Beziehung

$$(4) \qquad \sqrt{p}=2^{\frac{p-1}{2}}\sin\frac{2\pi}{p}\sin 2\frac{2\pi}{p}\sin 3\frac{2\pi}{p} \ . \ . \ . \ \sin\frac{p-1}{2}\frac{2\pi}{p},$$

wo die sin auf der rechten Seite wesentlich positive Werte haben, also auch auf der linken Seite das Vorzeichen der Wurzel positiv zu nehmen ist.

Im folgenden wollen wir nun die beiden Fälle $p=4n+1$ und $p=4n+3$ unterscheiden.

Es sei also

I. p von der Form $4n+1$.

Dann lässt sich die frühere Formel

$$\sum_{s=1}^{s=p-1}\left(\frac{s}{p}\right)e^{s\frac{2\pi i}{p}}=\varepsilon\sqrt{p}$$

in folgender Weise vereinfachen.

Bezeichnet a einen quadratischen Rest nach dem Modul p,

so ist wegen $p=4n+1$ auch $-a$ Rest; ist aber b ein quadratischer Nichtrest, so ist auch $-b$ Nichtrest. Schreibt man also obige Summe einmal in richtiger Reihenfolge hin, das andere Mal in umgekehrter und dividiert die Summe von je zwei unter einanderstehenden Gliedern auf der linken Seite und ebenso die rechte Seite durch 2. so erhält man:

$$\sum_{s=1}^{s=p-1} \left(\frac{s}{p}\right) \cos s\frac{2\pi}{p} = \varepsilon \sqrt{p}$$

oder wegen der Gleichung (4)

$$\sum_{s=1}^{s=p-1} \left(\frac{s}{p}\right) \cos s\frac{2\pi}{p} = \varepsilon\, 2^{\frac{p-1}{2}} \sin \frac{2\pi}{p} \sin 2\frac{2\pi}{p} \sin 3\frac{2\pi}{p} \ldots \sin\frac{p-1}{2}\frac{2\pi}{p}.$$

Wir betrachten nun das Product

$$f(x)=2^{\frac{p-1}{2}} \sin x \,.\, \sin 2x \,.\, \sin 3x \ldots \sin\frac{p-1}{2}x$$

oder

$$f(x)=2^{\frac{p-1}{2}} \frac{e^{ix}-e^{-ix}}{2i} \cdot \frac{e^{2ix}-e^{-2ix}}{2i} \cdot \frac{e^{3ix}-e^{-3ix}}{2i} \ldots \frac{e^{\frac{p-1}{2}ix}-e^{-\frac{p-1}{2}ix}}{2i}.$$

Führt man in dem letzten Ausdrucke die Multiplication auf der rechten Seite aus, so muss jedem Term $\pm e^{imx}$ ein Term $\pm e^{-imx}$ entsprechen. Denn da die allgemeine Form der Glieder

$$\pm e^{(\pm 1 \pm 2 \pm 3 \pm \ldots \pm \frac{p-1}{2})ix}$$

ist, wo das Vorzeichen vor dem ganzen Ausdrucke gleich dem Producte der Vorzeichen der einzelnen Glieder des Aggregates im Exponenten ist, so erhält man durch Vertauschung der Vorzeichen im Exponenten einen neuen Term, in welchem zwar der Exponent entgegengesetztes Vorzeichen hat, nicht aber auch der

ganze Ausdruck, da die Anzahl der Glieder im Exponenten eine gerade ist. Demnach stellt sich unser Product als eine Summe der cosinus der Vielfachen von x dar. Wir können also auch schreiben

$$f(x)=A_0+A_1\cos x+A_2\cos 2x+A_3\cos 3x+\ldots A_n\cos nx,$$

wo A_0, A_1, A_2 . . . A_n ganze Zahlen sind. Fassen wir nun alle Glieder zusammen, für welche die Vielfachen im Argumente der cosinus einer und derselben Zahl nach dem Modulus p congruent sind, so erhalten wir

$$f(x) = A_0$$

$$+A_1\cos x + A_{p+1}\cos(p+1)x + A_{2p+1}\cos(2p+1)x + \ldots$$

$$+A_2\cos 2x + A_{p+2}\cos(p+2)x + A_{2p+2}\cos(2p+2)x + \ldots$$

$$+A_3\cos 3x + A_{p+3}\cos(p+3)x + A_{2p+3}\cos(2p+3)x + \ldots$$

. . . . . .

. . . . . .

$$+A_{p-1}\cos(p-1)x + A_{2p-1}\cos(2p-1)x + A_{3p-1}\cos(3p-1)x + \ldots$$

$$+A_p\cos px + A_{2p}\cos 2px + A_{3p}\cos 3px + \ldots\ldots$$

Nun wissen wir aber, dass für $x = \frac{2\pi}{p}$

$$f\left(\frac{2\pi}{p}\right) = \sqrt{p}$$

wird. Dabei reduciert sich die rechte Seite auf

$$A_0 + A_p + A_{2p} + A_{3p} + \ldots\ldots$$

$$+(A_1 + A_{p+1} + A_{2p+1} + A_{3p+1} + \ldots)\cos\frac{2\pi}{p}$$

$$+(A_2+A_{p+2}+A_{2p+2}+A_{3p+2}+\ldots)\cos 2\frac{2\pi}{p}$$

. . . . . .

. . . . . .

$$+(A_{p-1}+A_{2p-1}+A_{3p-1}+A_{4p-1}+\ldots)\cos(p-1)\frac{2\pi}{p}\ \ldots$$

Nun ist, wenn wir wieder die p^{te} Einheitswurzel $e^{\frac{2\pi i}{p}}$ mit r bezeichnen,

$$r^{p-1}+r^{p-2}+r^{p-3}+\ldots+r^2+r+1=0,$$

also

$$\frac{r+r^{p-1}}{2}+\frac{r^2+r^{p-2}}{2}+\frac{r^3+r^{p-3}}{2}+\ldots+\frac{r^{p-1}+r}{2}=-1,$$

somit

$$A_0+A_p+A_{2p}+A_{3p}+\ldots=$$

$$-(A_0+A_p+A_{2p}+A_{3p}+\ldots)\left(\frac{r+r^{p-1}}{2}+\frac{r^2+r^{p-2}}{2}+\ldots\frac{r^{p-1}+r}{2}\right).$$

Setzen wir ferner noch für $\cos n\frac{2\pi}{p}$ den ihm gleichen Wert $\frac{r^n+r^{p-n}}{2}$, so erhalten wir für $\sqrt{p}$ folgende Normalform:

$$\sqrt{p}=\left[A_1+A_{p+1}+A_{2p+1}+\ldots-(A_0+A_p+A_{2p}+\ldots)\right]\frac{r+r^{p-1}}{2}$$

$$+\left[A_2+A_{p+2}+A_{2p+2}+\ldots-(A_0+A_p+A_{2p}+\ldots)\right]\frac{r^2+r^{p-2}}{2}$$

. . . . . .

. . . . . .

$$+\left[A_{p-1}+A_{2p-1}+A_{3p-1}+\ldots-(A_0+A_p+A_{2p}+\ldots)\right]\frac{r^{p-1}+r}{2}.$$

Da aber auch nach dem Früheren

$$\varepsilon \sqrt{p} = \sum_{s=1}^{s=p-1} \left(\frac{s}{p}\right) \cos s\frac{2\pi}{p}$$

$$= \left(\frac{1}{p}\right)\frac{r+r^{p-1}}{2} + \left(\frac{2}{p}\right)\frac{r^2+r^{p-2}}{2} + \ldots + \left(\frac{p-1}{p}\right)\frac{r^{p-1}+r}{2}$$

ist, so ergiebt sich wegen der Identität beider Normalformen allgemein

$$A_\nu + A_{p+\nu} + A_{2p+\nu} + \ldots = \varepsilon\left(\frac{r}{p}\right) + A_0 + A_p + A_{2p} + \ldots$$

$A_0 + A_p + A_{2p} + \ldots$ ist aber gleich 0, denn setzt man in der obigen Entwickelung von f(x) für x den Wert 0, so erhält man

$$f(o) = 0 = A_0 + A_p + A_{2p} + A_{3p} + \ldots$$

$$+ (A_1 + A_{p+1} + A_{2p+1} + \ldots)$$

$$+ (A_2 + A_{p+2} + A_{2p+2} + \ldots)$$

$$\ldots\ldots\ldots\ldots$$

$$+ (A_{p-1} + A_{2p-1} + A_{3p-1} + \ldots)$$

$$= p(A_0 + A_p + A_{2p} + A_{3p} + \ldots) + \varepsilon \sum_{s=1}^{s=p-1} \left(\frac{s}{p}\right)$$

$$= p\,(A_0 + A_p + A_{2p} + A_{3p} + \ldots).$$

Hieraus folgt unmittelbar die Richtigkeit unserer Behauptung.

Es ist demnach

$$A_\nu + A_{p+\nu} + A_{2p+\nu} + \ldots = \varepsilon\left(\frac{\nu}{p}\right).$$

Wir differentieren jetzt den Ausdruck

$$2^{\frac{p-1}{1}} \sin x \sin 2x \sin 3x \ldots \sin\frac{p-1}{2}x = A_0$$

$$+A_1 \cos x + A_{p+1}\cos(p+1)x + A_{2p+1}\cos(2p+1)x + \ldots$$

$$+A_2 \cos 2x + A_{p+2}\cos(p+2)x + A_{2p+2}\cos(2p+2)x + \ldots$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$+A_{p-1}\cos(p-1)x + A_{2p-1}\cos(2p-1)x + A_{3p-1}\cos(3p-1)x + \ldots$$

$$+A_p \cos px + A_{2p}\cos 2px + A_{3p}\cos 3px + \ldots\ldots$$

$\frac{p-1}{2}$mal nach einander und setzen nach Ausführung der Rechnung $x = 0$.

Es bleibt dann links nur

$$2^{\frac{p-1}{2}}(1.\,2.\,3.\,4\ldots\ldots\frac{p-1}{2})^2$$

stehen, während die rechte Seite

$$(-1)^{\frac{p-1}{4}}\left\{\begin{array}{l} A_1 + A_{p+1}(p+1)^{\frac{p-1}{2}} + A_{2p+1}(2p+1)^{\frac{p-1}{2}} + \ldots \\ +A_2 2^{\frac{p-1}{2}} + A_{p+2}(p+2)^{\frac{p-1}{2}} + A_{2p+2}(2p+2)^{\frac{p-1}{2}} + \ldots \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ +A_{p-1}(p-1)^{\frac{p-1}{2}} + A_{2p-1}(2p-1)^{\frac{p-1}{2}} + A_{3p-1}(3p-1)^{\frac{p-1}{2}} + \ldots \\ +A_p p^{\frac{p-1}{2}} + A_{2p}(2p)^{\frac{p-1}{2}} + A_{3p}(3p)^{\frac{p-1}{2}} + \ldots \end{array}\right\}$$

wird.

Demnach ist die rechte Seite nach dem Modulus p

$$\equiv(-1)^{\frac{p-1}{4}}\left\{\begin{array}{l} \left(\frac{1}{p}\right)(A_1 + A_{p+1} + A_{2p+1} + \ldots) \\ +\left(\frac{2}{p}\right)(A_2 + A_{p+2} + A_{2p+2} + \ldots) \\ +\left(\frac{3}{p}\right)(A_3 + A_{p+3} + A_{2p+3} + \ldots) \\ \ldots\ldots\ldots\ldots \\ +\left(\frac{p-1}{p}\right)A_{p-1} + A_{2p-1} + A_{3p-1} + \ldots) \end{array}\right\}.$$

Nun war aber

$$A_\nu + A_{p+\nu} + A_{2p+\nu} + \ldots = \varepsilon \left(\frac{\nu}{p} \right),$$

also ist die rechte Seite auch

$$\equiv (-1)^{\frac{p-1}{4}} \varepsilon \; (p-1) \equiv (-1)^{\frac{p+3}{4}} \cdot \varepsilon \pmod{p}.$$

Auf der linken Seite ist aber

$$2^{\frac{p-1}{2}} \equiv \left(\frac{2}{p}\right) \pmod{p}$$

und $(1.\ 2.\ 3.\ 4.\ \ldots\ \frac{p-1}{2})^2 \equiv -1 \pmod{p}$,

da der Wilsonsche Satz

$$1.\ 2.\ 3.\ 4.\ \ldots\ (p-1) \equiv -1 \pmod{p}$$

sich leicht umformen lässt in

$$1.\ 2.\ 3.\ 4.\ \ldots\ \frac{p-1}{2} \left(p-\frac{p-1}{2}\right) \left(p-\frac{p-3}{2}\right) \ldots (p-2)(p-1) \equiv -1 \pmod{p}$$

oder wegen

$$p-\nu \equiv -\nu \pmod{p}$$

in

$$\left(1.\ 2.\ 3.\ 4.\ \ldots\ \frac{p-1}{2}\right)^2 \equiv -1 \pmod{p}.$$

Endlich ergiebt sich noch leicht aus dem quadratischen Character der Zahl 2 für den Fall $p=4n+1$

$$(-1)^{\frac{p+3}{4}} \equiv -\left(\frac{2}{p}\right) \pmod{p}.$$

Demnach ist das Schlussresultat für den Fall $p=4n+1$

$$\varepsilon = +1.$$

II. Der Fall $p=4n+3$ lässt sich in ähnlicher Weise erledigen; nur wird in mancher Hinsicht die Entwickelung noch einfacher. Das Schlussresultat bleibt aber dasselbe, so dass in allen Fällen das Vorzeichen der Gaussischen Summen positiv zu nehmen ist.

2.

Bei einer genaueren Analyse des eben gegebenen Beweises erkennt man leicht, dass der eigentliche Angelpunkt desselben die $\frac{p-1}{2}$fache Differentiation ist. Das gleiche Mittel kann nun auch, wie schon früher erwähnt wurde, dazu dienen, den ersten der von *Kronecker* gegebenen Beweise einfacher und übersichtlicher zu gestalten.

Wir knüpfen an die nach dem Vorhergehenden unschwer zu beweisende Identität

$$\sum r^a - \sum r^b = (-1)^n \varepsilon \prod_{h=1}^{h=\frac{p-1}{2}} (r^h - r^{-h})$$

an, wo ε das zu bestimmende Vorzeichen

und $n = \frac{p-3}{4}$ für $p = 4n+3$

$n = \frac{p-1}{4}$ für $p = 4n+1$

ist. Die a bedeuten ein vollständiges System quadratischer Reste und entsprechend die b ein vollständiges System quadratischer Nichtreste.

In allen Productenausdrücken der rechten Seite, in denen $h < \frac{p}{4}$ ist, heben wir r^{-h} heraus, in allen andern, in denen $h < \frac{p}{4}$ ist, dagegen r^h. Das Product auf der rechten Seite nimmt dann die Form

$$\prod_{h=1}^{h=n} r^{-h} (r^{2h} - 1) \prod_{h=n+1}^{h=\frac{p-1}{2}} r^h (1 - r^{p-2h})$$

an, sodass sich nach einigen leichten Umformungen ergiebt

$$\sum r^a - \sum r^b = (-1)^{\frac{p-1}{2}} \varepsilon r^m \prod_{h=1}^{h=\frac{p-1}{2}} (r^h - 1),$$

wo m eine ganze Zahl bedeutet, deren Bestimmung zwar leicht, aber für das Folgende nicht nötig ist.

Diese Relation lehrt nun, weil der Summenausdruck und der Productenausdruck bis auf das Vorzeichen gleich sind, dass die Gleichung

$$\sum x^a - \sum x^b - (-1)^{\frac{p-1}{2}} \varepsilon x^m \prod_{h=1}^{h=\frac{p-1}{2}} (x^h - 1) = 0$$

mit offenbar ganzzahligen Coeffizienten für $x = r, r^2, r^3 \ldots r^p$ erfüllt sein muss, also sich durch $x^p - 1$ ohne Rest teilen lassen muss.

Demnach ist

$$\sum x^a - \sum x^b - (-1)^{\frac{p-1}{2}} \varepsilon x^m \prod_{h=1}^{h=\frac{p-1}{2}} (x^h - 1) = (x^p - 1) . F(x),$$

wo F (x) eine ganze algebraische Function von x mit ganzzahligen Coefficienten ist.

Wir wollen nun die linke und die rechte Seite $\frac{p-1}{2}$mal nach einander differentieren, dabei aber jedesmal nach Ausführung einer Differentiation beide Seiten mit x multiplicieren. In dem Schlussresultate setzen wir $x = 1$.

Der Summenausdruck auf der linken Seiten ergiebt dann

$$\sum a^{\frac{p-1}{2}} - \sum b^{\frac{p-1}{2}}.$$

Ebenso soll in dem Productenausdrucke nach $\frac{p-1}{2}$facher Differentiation und jedesmaliger Multiplication mit x für x der Wert 1

gesetzt werden, es brauchen also nach Ausführung der Rechnung nur solche Glieder beibehalten zu werden, in denen Factoren von der Form (x^h-1) nicht mehr vorkommen. So ergiebt sich leicht, dass nach der ersten Differentiation nur auf die $\frac{p-1}{2}$ Glieder Rücksicht zu nehmen ist, in denen $\frac{p-3}{2}$ Factoren (x^h-1) vorkommen, nach der zweiten Differentiation nur auf die $\frac{p-1}{2}\cdot\frac{p-3}{2}$ Glieder, in denen $\frac{p-5}{2}$ Factoren (x^h-1) vorkommen usw. Nach der $\frac{p-1}{2}$ten Differentiation hat man $\frac{p-1}{2}\cdot\frac{p-3}{2}\cdot\frac{p-5}{2}\ \ldots\ 3.\ 2.\ 1$ Glieder, die dadurch entstanden sind, dass in dem Productenausdruck jeder Factor einmal differentiert worden ist, so dass jedes Glied aus dem Zahlenfactor $1.\ 2.\ 3.\ \ldots\ \frac{p-1}{2}$ und einer gewissen Potenz von x besteht. Diese $1.\ 2.\ 3.\ \ldots\ \frac{p-1}{2}$ Glieder haben also für $x=1$ die Summe $(1.\ 2.\ 3.\ 4.\ \ldots\ \frac{p-1}{2})^2$. Die rechte Seite endlich ergiebt bei der Differentiation der Reihe nach

$$(x^p-1)\ F'(x)+p\,x^{p-1}F(x),$$

also nach Multiplication mit x

$$(x^p-1)\ x\,F'(x)+p\,x^pF(x),$$

dann

$$(x^p-1)\,x\,F''(x)+(x^p-1)\,F'(x)+2p\,x^p\,F'(x)+p^2x^{p-1}F(x)$$

u. s. w.

Setzt man also, nachdem man diese Operation $\frac{p-1}{2}$ mal wiederholt hat, $x=1$, so behält man auf der rechten Seite eine durch p teilbare Zahl übrig; demnach muss auch die ganze linke Seite durch p teilbar sein, oder es muss

$$\sum a^{\frac{p-1}{2}}-\sum b^{\frac{p-1}{2}}-(-1)^{\frac{p-1}{2}}\varepsilon\,(1.\ 2.\ 3.\ 4.\ \ldots\ \frac{p-1}{2})^2\equiv 0\ (\mathrm{mod.}\,p)$$

sein oder, da

$$a^{\frac{p-1}{2}}\equiv 1\ (\mathrm{mod.}\ p)$$

$$b^{\frac{p-1}{2}}\equiv -1\ (\mathrm{mod.}\ p)$$

und

$$(1.\ 2.\ 3.\ 4.\ \ldots\ \frac{p-1}{2})^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p}$$

ist, endlich

$$\varepsilon \equiv 1 \pmod{p}.$$

Da aber ε nur die beiden Werte $+1$ und -1 haben kann, so ergiebt sich als Schlussresultat

$$\varepsilon = 1.$$

Freilich ist damit der Satz nur für Primzahlen p bewiesen; wie aber schon bemerkt, lässt sich der Satz unter Benutzung des Reciprocitätsgesetzes in der Lehre von den quadratischen Resten auch für beliebige ungerade Zahlen P ohne quadratischen Teiler als richtig nachweisen, sodass sich die Formeln (2) und (3) in

$$\sum_{m=1}^{m=P-1} \left(\frac{m}{P}\right) e^{m\frac{2h\pi i}{P}} = \left(\frac{h}{P}\right) i^{\left(\frac{P-1}{2}\right)^2} \sqrt{P} \tag{5}$$

und

$$\sum_{m=0}^{m=P-1} e^{m^2\frac{2h\pi i}{P}} = \left(\frac{h}{P}\right) i^{\left(\frac{P-1}{2}\right)^2} \sqrt{P} \tag{6}$$

vereinfachen, wo in beiden Formeln das Vorzeichen von $\sqrt{P}$ durchaus positiv zu nehmen ist.

II. Abschnitt.

Einige Anwendungen der Gaussischen Summen auf die Zahlentheorie und die Lehre von der Kreisteilung.

4.

Aus der Identität

$$\sum_r^a - \sum_r^b = (-1)^{\left[\frac{p}{4}\right]} \prod_{h=1}^{h=\frac{p-1}{2}} (r^h - r^{-h}), \tag{7}$$

wo $\left[\frac{p}{4}\right]$ die grösste in $\frac{p}{4}$ enthaltene ganze Zahl bedeutet, kann man nun zunächst einen bemerkenswerten Satz der höheren Arithmetik ableiten. Führt man nämlich die Multiplication auf der rechten Seite aus, so hat der allgemeine Term die Form

$$\pm r^{\pm 1 \pm 2 \pm 3 \pm 4 \ldots \frac{\pm p-1}{2}},$$

wo das Vorzeichen von r gleich dem Producte der Vorzeichen von 1, 2, 3 u. s. w. ist. Schreibt man dann alle Terme zusammen, deren Exponenten einer und derselben Zahl nach dem Modulus p congruent sind, so müssen sich alle Terme bis auf einen forthehen, und zwar lehrt der Anblick der obigen Gleichung, dass folgender Satz bestehen muss:

Bezeichnet p eine Primzahl und bildet man durch entsprechende Wahl der Vorzeichen alle möglichen Combinationen

$$\pm 1 \pm 2 \pm 3 \pm 4 \ldots \pm \frac{p-1}{2},$$

die einer und derselben Zahl m nach dem Modulus p con-

gruent sind, so ist

$$\left(\frac{m}{p}\right) = (-1)^{\left[\frac{p}{4}\right]} \{A-B\},$$

wo A die Anzahl derjenigen Combinationen ist, in denen eine gerade Anzahl negativer Summanden vorkommt, während B die Anzahl der übrigen Combinationen ist.

So sind z. B. nach dem Modulus 11 folgende Combinationen der Zahl 5 congruent:

$$+1+2+3+4-5$$

$$-1+2+3-4+5$$

$$+1-2-3+4+5,$$

demnach

$$A = 2$$

$$B = 1,$$

und wirklich ist

$$\left(\frac{5}{11}\right) = (-1)^{\left[\frac{11}{4}\right]} (2-1) = 1.$$

Zu einem arithmetischen Beweise dieses Satzes kann man mit Hilfe ähnlicher Betrachtungen gelangen, wie sie *Cauchy* bei seinem zweiten Beweise für die Gaussischen Summen angestellt hat: im übrigen wird aber jeder selbständige Beweis des obigen Satzes zu einem neuen Beweise des berühmten Problems der Wertbestimmung der Gaussischen Summen führen. Es wäre daher sehr zu wünschen, wenn die obige Beziehung noch auf andere Weise bewiesen werden würde.

5.

Eine weitere interessante Anwendung unserer Untersuchungen auf die Zahlentheorie und die Lehre von der Kreisteilung ist folgende. Es sei

$$P = p\, p'\, p'' \ldots$$

eine ungerade, durch kein Quadrat (ausser 1) teilbare ganze Zahl.

Aus den Wurzeln der Gleichung

$$x^P - 1 = 0$$

mögen alle diejenigen ausgesondert werden, die nicht primitive Wurzeln sind. Es bleibt dann eine Gleichung übrig, deren Grad gleich der Anzahl der in der Reihe

$$1, 2, 3, 4, \ldots P-1$$

enthaltenen relativen Primzahlen zu P ist. In betreff der genaueren Entwickelungen müssen wir aber auf *Dirichlets* Vorlesungen über Zahlentheorie, herausgegeben von *R. Dedekind*, verweisen; daselbst ist pag. 363 u. ff. der Nachweis geführt, dass die Gleichung, welche sämtliche primitive Wurzeln enthält, die Form

$$\frac{\prod(x^{\mu_1}-1)}{\prod(x^{\mu_2}-1)}$$

hat, wo die Productenzeichen sich auf sämtliche μ_1 und μ_2 der Entwickelung

$$(p-1)(p'-1))p''-1) \ldots = \Sigma\mu_1 - \Sigma\mu_2$$

beziehen.

Dieselben Wurzeln können aber auch als Potenzen r^k einer einzigen primitiven Wurzel

$$r = e^{\frac{2\pi i}{P}}$$

dargestellt werden, wo k relative Primzahl zu P sein muss, und zwar ist für die eine Hälfte dieser Wurzeln

$$\left(\frac{k}{p}\right) = +1,$$

für die andere Hälfte

$$\left(\frac{k}{p}\right) = -1.$$

Die primitiven Wurzeln des ersten Complexes, die entsprechend unseren früheren Bezeichnungen mit

$$r^{a}$$

bezeichnet sein mögen, sind dann sämtlich Wurzeln der Gleichung

$$A(x) = \prod (x - r^{a}) = 0,$$

und die des zweiten Complexes, r^{b}, sämtlich Wurzeln der Gleichung

$$B(x) = \prod (x - r^{b}) = 0,$$

sodass zunächst

$$A(x) \cdot B(x) = \frac{\prod (x^{\mu_1} - 1)}{\prod (x^{\mu_2} - 1)}$$

sein muss.

Mit Hilfe der Newtonschen Formeln über die Potenzsummen der Gleichungswurzeln und unter Benutzung der obigen Formeln für die Gaussischen Summen lässt sich dann leicht, wie an der oben citierten Stelle geschehen ist, nachweisen, dass

$$2A(x) = Y(x) - Z(x)\, i^{\left(\frac{P-1}{2}\right)^2} \sqrt{P}$$

$$2B(x) = Y(x) + Z(x)\, i^{\left(\frac{P-1}{2}\right)^2} \sqrt{P}$$

ist, wo $Y(x)$ und $Z(x)$ ganze Functionen bedeuten, deren sämtliche Coefficienten rationale ganze Zahlen sind.

Für den speciellen Fall einer Primzahl p ist dieser Satz schon von Gauss bewiesen worden [1]).

Wir knüpfen an den allgemeinen Satz an. Aus diesem folgt unmittelbar

[1]) Disq. Arith. art. 357.

$$\frac{\prod(x-r^{a})}{\prod(x-r^{b})} = \frac{Y(x)-i^{\left(\frac{P-1}{2}\right)^{2}}Z(x)\sqrt{P}}{Y(x)+i^{\left(\frac{P-1}{2}\right)^{2}}Z(x)\sqrt{P}}$$

oder durch Logarithmierung

$$\sum \ln(x-r^{a}) - \ln\sum(x-r^{b}) = \ln\frac{Y(x)-i\left(\frac{P-1}{2}\right)Z(x)\sqrt{P}}{Y(x)+i^{\left(\frac{P-1}{2}\right)^{2}}Z(x)\sqrt{P}}.$$

Differentiert man nun auf beiden Seiten nach x, so ergiebt sich zunächst

$$\sum\frac{1}{x-r^{a}} - \sum\frac{1}{x-r^{b}} = -2i^{\left(\frac{P-1}{2}\right)^{2}}\sqrt{P}\;\frac{Y(x)Z'(x)-Z(x)Y'(x)}{Y^{2}(x)-(-1)^{\frac{P-1}{2}}PZ^{2}(x)}.$$

Mit Rücksicht auf die Formel

$$\frac{1}{x-r^{k}} = \frac{1}{x}\left(1+\frac{r^{k}}{x}+\frac{r^{2k}}{x^{2}}+\cdots+\frac{r^{(P-1)k}}{x^{P-1}}\right)+\frac{1}{x^{P}(x-r^{k})}$$

wird aber die linke Seite gleich

$$\frac{1}{x}\left(\sum r^{a}-\sum r^{b}\right)\left\{\frac{1}{x}+\left(\frac{2}{P}\right)\frac{1}{x^{2}}+\left(\frac{3}{P}\right)\frac{1}{x^{3}}+\cdots+\left(\frac{P-1}{P}\right)\frac{1}{x^{P-1}}\right\}$$

$$+\frac{1}{x^{P}}\left\{\sum\frac{1}{x-r^{a}}-\sum\frac{1}{x-r^{b}}\right\}.$$

Demnach

$$\frac{1}{x}\left\{\sum r^{a}-\sum r^{b}\right\}\left\{\frac{1}{x}+\left(\frac{2}{P}\right)\frac{1}{x^{2}}+\left(\frac{3}{P}\right)\frac{1}{x^{3}}+\cdots+\left(\frac{P-1}{P}\right)\frac{1}{x^{P-1}}\right\}$$

$$=\frac{x^{P}-1}{x^{P}}\left\{\sum\frac{1}{x-r^{a}}-\sum\frac{1}{x-r^{b}}\right\}$$

oder nach Formel (5)

$$\frac{1}{x}\, i^{\left(\frac{P-1}{2}\right)^2} \sqrt{P} \left\{ x^{P-1} + \left(\frac{2}{P}\right) x^{P-2} + \left(\frac{3}{P}\right) x^{P-3} + \ldots \left(\frac{P-1}{P}\right) x \right\}$$

$$= -\left(x^P - 1\right) 2\, i^{\left(\frac{P-1}{2}\right)^2} \sqrt{P}\ \frac{Y(x)Z'(x) - Z(x)Y'(x)}{Y^2(x) - (-1)^{\frac{P-1}{2}} P Z^2(x)},$$

also

$$x^{P-1} + \left(\frac{2}{P}\right) x^{P-2} + \left(\frac{3}{P}\right) x^{P-3} + \ldots \left(\frac{P-1}{P}\right) x$$

$$= -2x(x^P - 1)\, \frac{Y(x)\, Z'(x) - Z(x)\, Y'(x)}{Y^2(x) - (-1)^{\frac{P-1}{2}} P Z^2(x)}.$$

Nun ist aber

$$Y^2(x) - (-1)^{\frac{P-1}{2}} P Z^2(x) = 4 \frac{\prod (x^{\mu_1} - 1)}{\prod (x^{\mu_2} - 1)},$$

demnach folgt als Endresultat

$$(8)\quad x^{P-1} + \left(\frac{2}{P}\right) x^{P-2} + \left(\frac{3}{P}\right) x^{P-3} + \ldots \left(\frac{P-1}{P}\right) x$$

$$= -\frac{2x(x^P - 1)}{4} \frac{\prod (x^{\mu_2} - 1)}{\prod (x^{\mu_1} - 1)}\ (Y(x)Z'(x) - Z(x)Y'(x).$$

6.

Aus dieser Formel lassen sich durch Specialisierungen einige wichtige Resultate ableiten.

Für eine Primzahl p ist zunächst

$$\mu_1 = p$$

$$\mu_2 = 1.$$

Demnach

$$x^{p-1} + \left(\frac{2}{p}\right) x^{p-2} + \left(\frac{3}{p}\right) x^{p-3} + \ldots + \left(\frac{p-1}{p}\right) x$$

$$= -\frac{x(x-1)}{2} \left\{ Y(x)\, Z'(x) - Z(x) Y'(x) \right\}.$$

Ist ferner p von der Form $4n+3$, so folgt unmittelbar, indem man

$$x = -1$$

setzt,

$$\sum_{a=1}^{\frac{p-1}{2}} \left(\frac{p-2a}{p}\right) - \sum_{a=1}^{\frac{p-1}{2}} \left(\frac{2a}{p}\right) = -2\left(\frac{2}{p}\right)\sum_{1}^{\frac{p-1}{2}} \left(\frac{a}{p}\right)$$

$$= -Y(-1)\,Z'(-1) + Z(-1)\,Y'(-1).$$

Nun ist aber für unseren Fall

$$4\,(x^{p-1}+x^{p-2}+x^{p-3}+ \ldots x^2+x+1) = Y^2(x)+pZ^2(x),$$

also für $x = -1$

$$4 = Y^2(-1) + p\,Z^2(-1).$$

Demnach muss $Z(-1) = 0$ sein und $Y(-1)$ kann nur den Wert $+2$ oder -2 haben.

Die Entscheidung darüber, welcher Wert der richtige ist, kann in folgender Weise getroffen werden.

Es ist

$$(x-1)^p = x^p - 1 - p\,.\,F(x),$$

wo $F(x)$ eine ganze Function von x mit ganzzahligen Coefficienten ist.

Demnach

$$x^p - 1 = (x-1)^p + p\ .\ F(x),$$

mithin

$$4(x^{p-1}+x^{p-2}+x^{p-3}+ \ldots x^2+x+1)\,(x-1) =$$
$$= (x-1)\,(Y^2(x)+pZ^2(x)) = 4(x-1)^p + 4p\,.\,F(x).$$

Lässt man in dieser Gleichung die Vielfachen von p weg, so wird

$$(x-1)\,Y^2(x) \equiv 4\,(x-1)^p \pmod{p},$$

folglich

$$Y^2(x) \equiv 4\,(x-1)^{p-1} \pmod{p}$$

und

$$Y(x) \equiv 2\,(x-1)^{\frac{p-1}{2}} \pmod{p}.$$

Demnach ist

$$Y(-1) \equiv 2\,(-2)^{\frac{p-1}{2}} \equiv -\,2\left(\frac{2}{p}\right) \pmod{p}$$

oder, da $Y(-1)$ nur die Werte $+2$ oder -2 haben kann,

$$Y(-1) = -\,2\left(\frac{2}{p}\right).$$

Unter Benutzung der eben erhaltenen Werte ergiebt sich so

$$-2\left(\frac{2}{p}\right)\sum_{1}^{\frac{p-1}{2}}\left(\frac{a}{p}\right) = +\,2\left(\frac{2}{p}\right) Z^{1}(-1)$$

oder

$$\sum_{1}^{\frac{p-1}{2}}\left(\frac{a}{p}\right) = -\,Z'(-1). \tag{9}$$

So ist z. B. für $p=11$

$$\sum_{1}^{5}\left(\frac{a}{p}\right) = 3$$

$$Z(x) = x^4 + x$$

$$Z'(x) = 4x^3 + 1.$$

Wirklich ist $-Z'(-1)$ ebenfalls gleich 3.

7.

Dasselbe Resultat nur mit einer kleinen Modification gilt auch für eine zusammengesetzte Zahl $P=4n+3$.

Ist nämlich

$$P = p'\,p\,p'' \ldots$$

und setzt man in der Gleichung (8) für x den Wert -1, so wird, weil die ungeraden Zahlen μ_1 und μ_2 in gleicher Anzahl

vorkommen, ähnlich wie früher

$$-2\left(\frac{2}{P}\right)\sum_{1}^{\frac{P-1}{2}}\left(\frac{a}{P}\right)=-Y(-1)\,Z'(-1)+Z(-1)\,Y'(-1)$$

oder

$$2\left(\frac{2}{P}\right)\sum_{1}^{\frac{P-1}{2}}\left(\frac{a}{P}\right)=Y(-1)\,Z'(-1)-Z(-1)\,Y'(-1).$$

Ebenso lässt sich beweisen, dass

$$Z(-1)=0$$

sein muss und $Y(-1)$ nur die Werte $+2$ oder -2 haben kann. Um auch hier die Entscheidung zu treffen, haben wir zunächst einen Hilfssatz zu entwickeln.

Es bezeichne

a den Complex aller relativen Primzahlen zu P, die $<\frac{P}{2}$ sind,

a' den Complex derselben Zahlen $<\frac{P}{4}$ und

a'' den Complex derselben Zahlen zwischen $\frac{P}{4}$ und $\frac{P}{2}$. Dann ist für $P=4n+3$

$$\sum\left(\frac{a}{P}\right)=\sum\left(\frac{2a'}{P}\right)+\sum\left(\frac{P-2a''}{P}\right)=\sum\left(\frac{2a'}{P}\right)-\sum\left(\frac{2a''}{P}\right)$$
$$=\left(\frac{2}{P}\right)\left\{\sum\left(\frac{a'}{P}\right)-\sum\left(\frac{a''}{P}\right)\right\}.$$

Mithin

$$\left(\frac{2}{P}\right)=\frac{\sum\left(\frac{a'}{P}\right)-\sum\left(\frac{a''}{P}\right)}{\sum\left(\frac{a'}{P}\right)+\sum\left(\frac{a''}{P}\right)}.$$

Ist also $\left(\frac{2}{P}\right)=1$, so muss $\sum\left(\frac{a''}{P}\right)=0$ sein,

und ist $\left(\frac{2}{P}\right)=-1$, so muss $\sum\left(\frac{a'}{P}\right)=0$ sein.

Auf jeden Fall ist aber, weil überhaupt die Anzahl aller Zahlen a gerade ist, für eine ungerade zusammengesetzte Zahl $P=4n+3$ die Anzahl der zwischen $\frac{P}{4}$ und $\frac{P}{2}$ liegenden relativen Primzahlen zu P stets eine gerade.

Setzt man nun in

$$2\,A(x) = 2\prod(x - r^a) = Y(x) - iZ(x)\sqrt{P}$$

oder in

$$2\,B(x) = 2\prod(x - r^b) = Y(x) + iZ(x)\sqrt{P}$$

für x den Wert -1, so muss wegen

$$Z(-1) = 0$$

$$Y(-1) = 2\prod(-1 - r^a) = 2\prod(-1 - r^b)$$

sein. Es ist also unter allen Umständen auch

$$Y(-1) = 2\prod(-1 - r^{2a}) = 2\prod(-1 - r^{2b})$$

oder, da unter dem Productenzeichen

$$\frac{p-1}{2}\,(p'-1)\,(p''-1)\,\ldots$$

Factoren vorkommen, d. h. eine gerade Anzahl,

$$Y(-1) = 2\prod(1 + r^{2a}) = 2\prod(1 + r^{2b}).$$

Hierfür kann man auch schreiben

$$Y(-1) = 2\prod\frac{r^{-a} + r^a}{r^{-a}} = 2\prod\frac{r^{-b} + r^b}{r^{-b}},$$

oder wegen

$$\prod(r^{-a}) = 1$$

und

$$\prod(r^{-b}) = 1$$

auch

$$Y(-1) = 2\prod(r^a + r^{-a}) = 2\prod(r^b + r^{-b}).$$

Somit folgt also, da

$$r = e^{\frac{2\pi i}{P}}$$

ist,

$$Y(-1) = 2\prod 2\cos a\frac{2\pi}{P} = 2\prod 2\cos b\frac{2\pi}{P}.$$

Dieser Ausdruck hat aber einen positiven oder negativen Wert, je nachdem die zwischen $\frac{P}{4}$ und $\frac{3P}{4}$ gelegenen Zahlen a oder b in gerader oder ungerader Anzahl vorkommen. Da nun

$$\left(\frac{-a}{P}\right) = -1$$

und

$$\left(\frac{-b}{P}\right) = +1$$

ist, so muss diese Zahl gleich der Anzahl der zwischen $\frac{P}{4}$ und $\frac{P}{2}$ liegenden relativen Primzahlen zu P sein. Nach dem eben entwickelten Hilfsatze ist aber diese Anzahl unter allen Umständen eine gerade; demnach

$$Y(-1) = 2.$$

Somit ergiebt sich als Schlussresultat

$$\sum_{1}^{\frac{P-1}{2}} \left(\frac{a}{P}\right) = \left(\frac{2}{P}\right) Z'(-1). \tag{10}$$

So ist z. B. für P = 35

$$Z(x) = x^{11} - x^{10} - x^9 + 3x^8 - 3x^7 + 3x^5 - 3x^4 + x^3 + x^2 - x$$
$$Z'(x) = 11x^{10} - 10x^9 - 9x^8 + 24x^7 - 21x^6 + 15x^4 - 12x^3 + 3x^2 + 2x - 1,$$

also

$$Z'(-1) = -6,$$

Demnach

$$\sum_{1}^{\frac{P-1}{2}} \left(\frac{a}{P}\right) = -\left(\frac{2}{P}\right) 6,$$

oder da

$$\left(\frac{2}{P}\right) = -1 \qquad \text{ist,}$$

$$\sum_{1}^{\frac{P-1}{2}} \left(\frac{a}{P}\right) = 6.$$

Von der Richtigkeit dieser Gleichung kann man sich leicht durch direkte Berechnung der Ausdrücke unter dem Summenzeichen überzeugen.

8.

Ähnliche Resultate lassen sich auch für Zahlen P von der Form $4n+1$ ableiten; wir sehen aber von einer ausführlichen Entwickelung dieser Beziehungen ab. Denn die wirkliche Berechnung der Ausdrücke wird auf dem hier eingeschlagenen Wege derartig weitläufig, dass sie nur für kleine Zahlen überhaupt durchführbar ist. Desto grösser ist aber das theoretische Interesse, auf das wir hier indessen nur hinweisen können. Von *Dirichlet* ist nämlich auf höchst merkwürdige Weise, indem er die Analysis mit der Zahlentheorie in Verbindung brachte, gezeigt worden, dass die obigen Summenausdrücke eng mit der Klassenanzahl der binären quadratischen Formen mit negativer Determinante zusammenhängen. Für positive Determinanten erhielt er wesentlich davon verschiedene Ausdrücke, in denen die beiden vor allen andern ausgezeichneten Auflösungen der Pellschen Gleichung eine Hauptrolle spielen, nämlich die Fundamentallösung der kleinsten Zahlen und die aus der Theorie der Kreisteilung sich ergebende Auflösung mit Hülfe der oben als $Y(x)$ und $Z(x)$ bezeichneten Functionen, welche Lösung zuerst von *Dirichlet* in einer kleinen Abhandlung: Über die Auflösung der Pellschen Gleichung durch Kreisfunktionen, angegeben worden ist. Das theoretische Interesse unserer Entwickelungen besteht also in dem Nachweise, dass

auch für den Fall einer negativen Determinante eine Beziehung zwischen der Klassenanzahl und den Functionen Y(x) und Z(x) besteht. Weil demnach diese Functionen eine grosse Rolle in der Zahlentheorie spielen, möge es zum Schlusse noch gestattet sein, hier eine Tafel beizufügen, welche die Werte der Coefficienten für alle in betracht kommenden Zahlen bis 101 incl. giebt.

Zur Erklärung der Bezeichnung diene, dass

$$Y(x) = y_0\, x^\tau + y_1\, x^{\tau-1} + y_2\, x^{\tau-2} + \ldots$$

$$Z(x) = z_0\, x^\tau + z_1\, x^{\tau-1} + z_2\, x^{\tau-2} + \ldots$$

ist, wo τ die Anzahl derjenigen Zahlen, bezeichnet, für welche $(\frac{a}{P}) = +1$ ist, d. h. $\tau = \frac{1}{2}(p-1)(p'-1)(p''-1)\ \ldots$, wo p, p′ p″ . . . die einzelnen in P aufgehenden Primzahlen bedeuten.

Zahl	Coefficient	Werte der einzelnen Coefficienten,											
		0	1	2	3	4	5	6	7	8	9	10	11
5	y	2	1	2									
	z	0	1	0									
7	y	2	1	−1	−2								
	z	0	1	1	0								
11	y	2	1	−2	2	−1	−2						
	z	0	1	0	0	1	0						
13	y	2	1	4	−1	4	1	2					
	z	0	1	0	1	0	1	0					
15	y	2	−1	−4	−1	2							
	z	0	1	0	−1	0							
17	y	2	1	5	7	4	7	5	1	2			
	z	0	1	1	1	2	1	1	1	0			
19	y	2	1	−4	3	5	−5	−3	4	−1	−2		
	z	0	1	0	−1	1	1	−1	0	1	0		
21	y	2	−1	5	−7	5	−1	2					
	z	0	1	−1	1	−1	1	0					
23	y	2	1	−5	−8	−7	−4	4	7	8	5	−1	−2
	z	0	1	1	0	−1	−2	−2	−1	0	1	1	0
29	y	2	1	8	−3	+1	−2	+3	9	3	−2	1	−3
	z	0	1	0	1	−1	0	1	1	1	0	−1	1
31	y	2	1	−7	−11	2	8	−3	−5	5	3	−8	−2
	z	0	1	1	−1	−2	0	1	−1	−1	1	0	−2
33	y	2	−1	8	5	2	14	2	5	8	−1	2	
	z	0	1	0	1	2	0	2	1	0	1	0	
35	y	2	−1	−9	13	−5	−13	24	−13	−5	13	−9	−1
	z	0	1	−1	−1	3	−3	0	3	−3	1	1	−1
37	y	2	1	10	−4	15	−5	17	−8	11	−4	11	−8
	z	0	1	0	2	−1	3	−1	2	−1	2	−1	2
39	y	2	−1	−10	−4	11	5	−4	5	11	−4	−10	−1
	z	0	1	0	−2	−1	1	0	−1	1	2	0	−1

deren Indices der Reihe nach:

12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
8	1	2												
0	1	0												
11	7	−1	−2											
−1	1	1	0											
2														
0														
17	−5	15	−4	10	1	2								
−1	3	−1	2	0	1	0								
2														
0														

Zahl	Coefficient	Werte der einzelnen Coefficienten.											
		0	1	2	3	4	5	6	7	8	9	10	11
41	y	2	1	11	16	14	29	30	22	36	34	20	34
	z	0	1	1	1	4	3	4	6	4	4	6	4
43	y	2	1	−10	6	16	−20	−4	27	−15	−7	17	−17
	z	0	1	0	−2	2	2	−4	1	3	−3	1	1
47	y	2	1	−11	−17	−9	6	29	37	20	−2	−16	−11
	z	0	1	1	−1	−3	−4	−3	1	4	4	2	−1
51	y	2	−1	−13	20	5	−46	38	26	−64	26	38	−46
	z	0	1	−1	−2	5	−2	−6	8	0	−8	6	2
53	y	2	1	14	−6	8	−14	−4	19	−12	24	−9	−11
	z	0	1	0	2	−2	0	0	−1	4	−2	1	1
55	y	2	−1	−14	−7	30	22	−26	−29	13	15	−8	15
	z	0	1	0	−3	−2	4	4	−3	−3	1	0	−1
57	y	2	−1	14	8	11	35	11	29	38	8	38	29
	z	0	1	0	2	3	1	5	3	2	6	2	3
59	y	2	1	−14	8	7	−35	22	12	−33	18	23	−29
	z	0	1	0	−2	3	−1	−4	4	−1	−4	3	1
61	y	2	1	16	−7	32	−20	63	−33	72	−54	89	−62
	z	0	1	0	3	−2	6	−3	9	−6	10	−7	12
65	y	2	−1	16	8	5	37	−6	6	43	−30	22	44
	z	0	1	0	2	3	−1	4	2	−3	6	0	−2
67	y	2	1	−16	9	33	−44	−18	79	−39	−48	75	−35
	z	0	1	0	−3	3	4	−8	1	9	−8	−1	7
69	y	2	−1	17	−25	35	−46	59	−40	29	−34	20	−7
	z	0	1	−1	3	−5	6	−5	6	−5	2	−2	3
71	y	2	1	−17	−26	−5	31	58	64	60	33	−29	−89
	z	0	1	1	−2	−5	−5	−2	2	6	11	13	9
73	y	2	1	19	28	61	106	158	251	322	442	544	652
	z	0	1	1	4	7	12	20	27	40	50	64	78
77	y	2	−1	19	−29	30	−56	35	23	−50	103	−141	94
	z	0	1	−1	3	−6	4	−3	1	8	−13	13	−12

deren Indices der Reihe nach:

12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
36	22	30	29	14										
4	6	4	3	4										
7	15	−27	4	20										
−3	3	1	−4	2										
11	16	2	−20	−37										
−1	2	4	4	1										
5	20	−13	−1	2	x									
−5	2	1	−1	0	y									
27	25	27	−11	−9										
−3	5	−3	1	1										
13	−29	−26	22	30										
3	3	−4	−4	2										
11	35	11	8	14										
5	1	3	2	0										
14	18	−29	29	−18	−14	29	−23	−18	33	−12				
4	4	−1	−1	4	−4	1	3	−4	−1	4				
88	−89	95	−81	95	−89	88	−62	89	−54	72				
−10	11	−11	13	−11	11	−10	12	−7	10	−6				
−34	44	22	−30	43	6	−6	37	5	8	16				
8	−2	0	6	−3	2	4	−1	3	2	0				
−14	69	−89	10	106	−106	−10	89	−69	14	35				
−8	5	5	−14	8	8	−14	5	5	−8	7	z			
20	−34	29	−40	59	−46	35	−25	17	−1	2	w			
−2	2	−5	6	−5	6	−5	3	−1	1	0				
−106	−91	−70	−44	−16	−3	3	16	44	70	91				
2	−3	−6	−8	−8	−7	−7	−8	−8	−6	−3				
783	868	983	1050	1113	1164	1156	1164	1113	1050	983				
89	104	113	124	131	134	138	134	131	124	113				
−18	−57	145	−189	145	−57	−18	94	−141	103	−50				
4	9	−17	19	−17	9	4	−12	13	−13	8				

Zahl	Coefficient	Werte der einzelnen Coefficienten,											
		0	1	2	3	4	5	6	7	8	9	10	11
79	y	2	1	—19	—29	24	69	4	—64	19	75	—67	-125
	z	0	1	1	—3	—6	1	8	0	—7	5	11	—9
83	y	2	1	—20	11	20	—65	58	42	-137	115	47	-223
	z	0	1	0	—3	4	—1	—8	12	—3	—13	21	—7
85	y	2	—1	21	—32	65	—98	159	-189	223	-250	287	-301
	z	0	1	—1	4	—7	12	—15	21	—25	28	—29	33
87	y	2	—1	—22	—10	47	44	—7	—25	—52	—64	38	101
	z	0	1	0	—4	—3	4	5	3	2	—6	—10	1
89	y	2	1	23	34	52	118	123	146	237	209	203	303
	z	0	1	1	4	8	8	15	20	17	25	29	21
91	y	2	—1	—23	34	44	-133	14	233	-176	-226	342	100
	z	0	1	—1	—4	8	3	—20	9	26	—28	—18	40
93	y	2	—1	23	—34	59	—91	104	—85	41	11	—52	65
	z	0	1	—1	4	—7	9	—10	9	—5	—1	6	—7
95	y	2	—1	—24	—12	40	67	49	—24	—87	—95	—83	—16
	z	0	1	0	—4	—4	1	7	10	5	—1	—7	—12
97	y	2	1	25	37	93	171	278	466	643	936	1219	1556
	z	0	1	1	5	9	17	30	40	69	92	125	160
101	y	2	1	26	—12	40	—65	33	9	40	49	-110	—4
	z	0	1	0	4	—4	3	—5	5	6	—3	0	—10

Beispielsweise ist für p=19

$$Y(x)=2x^9+x^8-4x^7+3x^6+5x^5-5x^4-3x^3+4x^2-x-2$$
$$Z(x)=\quad x^8-x^6+x^5+x^4-x^3+x$$

Für P=21

$$Y(x)=2x^6-x^5+5x^4-7x^3+5x^2-x+2$$
$$Z(x)=\quad x^5-x^4+x^3-x^2+x.$$

deren Indices der Reihe nach:

12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
81	166	−60	-137	87	110	-152	-148	148	152	-110	−87	137	60	-166
−17	8	18	−7	−13	14	14	−18	−18	14	14	−13	−7	18	8
184	62	-290	273	44	-343	319	7	-348	348	−7	-319	343	44	-273
−20	30	−12	23	40	−17	−23	43	-22	−22	43	23	17	40	−23
331	-377	425	-453	459	-453	425	-377	331	-301	287	-250	223	-189	159
−37	41	−45	49	−51	49	−45	41	−37	33	−29	28	25	21	15
17	−46	−46	46	17	101	38	−64	−52	−25	−7	44	47	−10	−22
9	4	0	−4	−9	−1	10	6	−2	−3	−5	−4	3	4	0
257	230	368	332	266	410	364	242	365	333	198	333	365	242	364
29	36	26	34	44	30	34	44	27	27	40	27	27	44	34
-385	22	327	−51	-272	21	254	21	-272	−51	327	22	-385	100	342
3	−38	5	31	−4	−27	0	27	4	−31	−5	38	−3	−40	18
−34	−13	74	-109	74	−13	−34	65	−52	11	41	−85	104	−91	59
4	3	−8	9	−8	3	4	−7	6	−1	−5	9	−10	9	−7
61	88	100	62	4	−69	-122	−69	4	62	100	88	61	−16	−83
−9	−4	2	8	10	9	0	−9	−10	−8	−2	4	9	12	7
1960	2295	2750	3111	3520	3930	4225	4632	4846	5114	5302	5347	5468	5347	5302
194	239	274	319	358	394	437	462	498	518	534	551	546	551	534
13	63	86	-166	−3	6	90	77	-185	19	53	76	66	-206	66
5	11	−4	0	−15	8	12	−5	−1	−13	11	14	−10	0	−10

Thesen.

1. Es ist anzunehmen und lässt sich auch durch das Gesetz von der Erhaltung der Energie beweisen, dass zwischen zwei Platten aus gleichem Metall, die in einer elektrolytischen Lösung desselben Metalls über einander angeordnet sind, eine elektromotorische Kraft auftreten muss, und zwar ist diese von der oberen Platte nach der unteren gerichtet.

2. Wird die Energie der Ebbe- und Flutbewegung zu mechanischen Arbeitsleistungen ausgenutzt, so geschieht dies auf Kosten der Rotationsenergie der Erde, während die Mond- und Sonnenanziehung nur soweit ins Spiel kommt, als sie überhaupt erst eine solche Ausnutzung der Bewegungsenergie der Erde möglich macht; man muss daher durchaus Herrn Dr. *Reche* beitreten, der diesen Standpunkt in der Zeitschrift „Prometheus" gegen Herrn Professor *Dziobek* verteidigt hat.

3. Es ist sehr wünschenswert, einen Unterschied zwischen den beiden Begriffen „Potentialdifferenz" und „elektromotorische Kraft" in der Art zu machen, dass man von einer Potentialdifferenz nur dann spricht, wenn freie elektrische Ladungen ins Spiel kommen, während unter elektromotorischer Kraft das Linienintegral der elektrischen Gesamtkraft längs der betrachteten Weglänge verstanden werden muss; denn es lassen sich Fälle denken und können auch durch den Versuch verwirklicht werden, in denen in einer Drahtleitung ein Strom von beliebiger Stärke beliebig lange fliessen kann, ohne dass durch einen Spannungsmesser zwischen zwei beliebigen Punkten der Strombahn eine Potentialdifferenz angezeigt wird.

Lebenslauf.

Der Verfasser, *Hermann Teege*, wurde am 2. Januar 1864 zu Schackendorf, Kr. Segeberg, Provinz Schleswig-Holstein, als Sohn eines Landmannes geboren und im evangelischen Glauben erzogen. Nachdem er zunächst die Wilhelmsschule (Realprogymnasium) zu Segeberg besucht hatte, kam er Ostern 1881 auf das Realgymnasium zu Rendsburg, das er Ostern 1883 mit dem Zeugnis der Reife verliess. Von Ostern 1884 bis Michaelis 1884 hörte er an der Universität zu Kiel Vorlesungen über Mathematik und Physik, erwarb sich Michaelis 1884 von der Königlichen Domschule (Gymnasium) zu Schleswig das Zeugnis der Reife eines Gymnasiums und ging dann auf die Universität zu Freiburg, von wo er Michaelis 1885 nach Kiel zurückkehrte. Hier bestand er am 22. Dezember 1888 vor der Königl. Wissenschaftl. Prüfungskommission das Examen pro fac. doc. und erwarb sich die Lehrbefähigung in Mathematik und Physik für die oberen Klassen, in Geographie, Chemie und Mineralogie für die mittleren Klassen einer höheren Lehranstalt. Das für Lehrer höherer Schulen vorgeschriebene Probejahr leistete er von Michaelis 1888 bis Michaelis 1889 an dem Königl. Gymnasium zu Flensburg ab und ist seitdem an der Oberrealschule zu Kiel, dem dortigen Gymnasium und der Kaiserl. Deckoffizierschule als Lehrer thätig gewesen.

Das Examen rigorosum bestand er am 13. Mai 1899.

Von seinen Lehrern ist er zu dauerndem Danke besonders den Herren Professoren Geh. Reg. Rat *G. Karsten*, Geh. Reg. Rat *L. Pochhammer* und *L. Weber* verpflichtet.

JUN 1

UNIVERSITY OF ILLINOIS-URBANA
512.74T22U C001
UEBER DIE P-1 / 2 GLIEDRIGEN GAUSSISCHEN
3 0112 017079184